METHOD AND APPARATUS FOR OVERCOMING A WATERMARK SECURITY SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the field of security, and in particular to providing access to copy-protected content material.

2. Description of Related Art

The protection of data is becoming an increasingly important area of security. In many situations, the authority to copy or otherwise process information is verified by evaluating the encoding of copy-protected material for particular characteristics. For example, copy-protected material may contain watermarks or other encodings that identify the material as being copy-protected, and also contains other encodings that identify whether this particular copy of the material is an authorized copy, and whether it can be copied again. For example, content material may be "watermarked" by an additional encoding process that adds a watermark that is not noticeable when the content material is being rendered in its appropriate form, but is detectable by a watermark detection process. Attempting to remove the watermark causes damage to the content material. When a watermark is detected, the content material is further evaluated to determine whether it is an authorized copy.

To assure that the content material is truly authorized, and that illicit content material has not been substituted for material that is authorized, the content material is often 'bound' to the parameter that is used to determine the authorization. For example, the authorization parameter may correspond to a hash value that is derived from the content material. To verify that the authorization corresponds to the proffered content material, a hash value of the proffered content material is determined, and compared to the original hash value contained in the authorization parameter. If the hash values do not match, further rendering of the content material ceases. Because the determination of a set of values that will produce a particular hash value is virtually impossible, in a cryptology sense, the comparison of hash values is commonly accepted as 'proof' that the original material and the proffered material are equivalent.

For large data sets, the data is partitioned into segments, and each segment is bound to an identifier that is used to determine the authorization to access the particular segment of the data set. To assure that each segment is bound to the data set, the identifier typically includes a common parameter, such as a data set identification number, that is associated with the particular data set.

Generally, the bandwidth available for encoding information into a watermark is extremely limited. A bandwidth of one bit per second of watermark is not uncommon. As such, the number of bits that available for encoding identifiers of segments and/or data sets is limited. For example, a typical segment of a CD is approximately fifteen seconds in duration. Thus, the identifier that is bound to each segment is limited to approximately fifteen bits. Increasing the length of each CD segment will increase the number of bits available for encoding in the watermark, but in any event, the number of unique identifiers of segments of a CD, or other media, will be finite.

BRIEF SUMMARY OF THE INVENTION

It is an object of this invention to disclose a method and apparatus for overcoming a security system that is limited by a finite number of unique identifiers. In particular, it is an object of this invention to disclose a method and apparatus that is configured to overcome a watermarking system having a limited information-carrying bandwidth.

These objects and others are achieved by creating a collection of authentic watermarked material, and providing a system that substitutes the authentic watermarked material to a watermark verification system in lieu of the content material that the watermark verification system is intended to verify. In security systems that are designed to verify the existence of authentic watermarked material, without regard to the actual content of the material, this substitution scheme will be successful. In security systems that are designed to verify the existence of an entirety of a data set in order to authorize the presentation of select material from the data set, the substitution of authentic watermarked material for the non-selected material will also be successful. A dictionary of expected watermarks for the data set is provided. When the security system requests the watermarked segments of the selected material, the selected material is presented; when the security system requests watermarked segments of the non-selected

material, the dictionary of expected watermarks is accessed, and the appropriate authentic watermarked material is presented from the stored collection.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in further detail, and by way of example, with reference to the accompanying drawings wherein:

FIG. 1 illustrates an example block diagram of a system that is configured to overcome a security procedure based on watermarks, in accordance with this invention.

FIG. 2 illustrates an example flow diagram of a system that is configured to overcome a security procedure based on watermarks, in accordance with this invention.

Throughout the drawings, the same reference numerals indicate similar or corresponding features or functions.

DETAILED DESCRIPTION OF THE INVENTION

For ease of reference and understanding, this invention is presented hereinafter in the context of a copy-protected CD that is organized into finite-length segments, although the principles of this invention are not limited to this particular media.

Copending U.S. patent application "Protecting Content from Illicit Reproduction by Proof of Existence of a Complete Data Set via Self-Referencing Sections", U.S. serial number 09/536,944, filed 28 March 2000 for Antonius A. M. Staring, Michael A. Epstein, and Martin Rosner, Attorney Docket US000040, incorporated by reference herein, addresses the illicit distribution of select content material from a collection of copy protected content material. Often, a song is 'ripped' from a CD and illicitly made available for distribution via the Internet. Each subsequent download of the song deprives the owner of the copyrights to the song of rightful royalties. A premise of this copending patent application is that the downloading of a song will be discouraged if the user is required to also download the entire contents of the CD. That is, due to bandwidth limitations and other factors, the illicit download of an entire CD is deemed to be substantially less likely than the illicit download of an individual song.

To verify that an entirety of the collection of content material is present when a particular song is presented for rendering, a compliant rendering device accesses other segments of the

collection, to verify their presence. To assure that these other sections belong to the same CD, an identifier in the watermark of each segment of the CD is bound to the segment.

As noted above, the bandwidth available for encoding information into a watermark is extremely limited, and the information-carrying capability of a typical watermark for a CD segment is limited to under twenty bits. Increasing the length of each CD segment will increase the number of bits available for encoding in the watermark, but in any event, the number of unique identifiers of segments of a CD, or other media, will be finite.

This invention is premised on the observation that, given the finite number of bits available for binding the watermark to the content material, it is feasible to create a collection of most, if not all, possible watermark values, with corresponding bound segments. This collection of authentic watermarked material may be the result of any of a variety of data collection and organizing efforts, such as an organized effort among a variety of illicit providers, or merely a categorization of segments of content material that a user has previously downloaded.

The invention is also premised on the observation that it is also feasible to determine the watermark value of each segment of a given CD. That is, given a watermark detector, common in the art, the watermark value of each segment of a CD can be read from an original, authorized, version of the CD. The list of watermarks for each CD can be widely, and legally, distributed. Specifically, the list of watermarks corresponding to each segment of a CD can be easily downloaded, without downloading the entirety of the contents of the CD.

If the watermarks cannot be easily read, a trial an error method can be used to find sections of music that will act as substitutes for other sections of music. First one would attempt to substitute one random section from an available collection. If a successful match is found, an identification of this substitute section is placed in a dictionary for later retrieval. Because the number of different watermark values is finite, after sufficient effort a dictionary will be constructed that can be used to substitute music from the collection for parts of a CD that are not present.

Any of a number of techniques, common in the art, can be used to access the dictionary for a given data set. For example, in the example of a CD data set, programs such as CDDB ("CD Data Base") are commonly available to identify the title and performer of each song on the CD,

and the like. When a section request appears, the system of this invention can determine which album-section is being requested and replace it with an appropriate substitute.

FIG. 1 illustrates a potential use of this collection of authentic watermarked segments 110 and the determined list 120 of watermarks corresponding to each segment of a watermarked data set to overcome a copy protection scheme based on watermarks.

In the example of FIG. 1, a rendering device 170 is configured to request sequential segments of content material to be rendered to the providing system, via a security device 160. Generally, the providing system is, for example, a CD player that contains an authorized copy of a CD, and the requested sequential segment correspond to the song that is to be rendered. In the security system of the aforementioned copending application, the security device 160 is configured to request the sequential segments from the providing system, and also to select segments from other songs on the CD, to verify that these other segments are also present at the providing system. By verifying the presence of other songs from the CD, the security device 160 verifies, to some degree of confidence, that the complete CD is present.

Alternatively, the system may be configured such that the providing system provides sequential segments directly to the security device 160 for forwarding to the rendering device 170, without requests from the rendering device. In this alternative arrangement, the security device 160 initiates requests for select segments of other songs on the CD to the providing system upon receipt of the unsolicited sequential segments from the providing system.

The example providing system 100 of this invention is configured to provide the watermarked segments 130 of desired material that has been ripped from a CD, and to satisfy segment requests for other material that had been on the CD from a collection of authentic watermarked segments 110 that have been previously downloaded by the user of the providing system 100.

The interface 150 receives the segment request 161 from the security device 160, and determines whether the segment corresponds to a segment in the ripped watermarked segments 130. If the requested segment 161 is not contained in the ripped watermark segments 130, the interface 150 forwards the segment request 161 to a substitution device 140. The substitution

device 140 determines the corresponding watermark for the requested segment 161, based on a 'dictionary' 120 that maps segment numbers to watermarks for the current content material. The substitution device 140 then retrieves an authentic watermarked segment corresponding to the requested segment request from the collection 110 of previously downloaded authentic watermarked segments. Note that the substituted watermarked segment from the collection 110 is not the segment that the security device 160 expects, in that it does not belong to the same data set as the ripped watermarked segments 130. However, because the substituted watermark and associated segment from the collection 110 has a duplicate watermark identifier, the security device 160 will conclude that it is the proper watermarked segment. Thus, the providing system will overcome the intended protection provided by the security device 160.

In a preferred embodiment of this invention, the downloaded ripped, and authentic, watermarked segments 130 are added to the collection 110 of previously downloaded authentic watermarked segments, thereby facilitating subsequent substitutions for other data sets.

Note that the dictionary, or mapping, 120, and the collection 110 need not be exhaustive to successfully overcome the intended protection provided by the security device 160. The security device 160 is typically configured to randomly sample the data set, to determine with some degree of confidence that the entire data set is present. Thus, the likelihood of an incomplete mapping 120 or collection 110 successfully overcoming the intended protection is dependent upon the likelihood that the security device will select a segment that is not included in either the mapping 120 or the collection 110. Thus, a providing system 100 of this invention may initially have a low success rate, but, with continued downloading of authentic watermarked segments, will continually increase its success rate.

FIG. 2 illustrates an example flow diagram of a system that is configured to overcome a security procedure based on watermarks in accordance with this invention. In this example, a user is assumed to have a subset of a data set, such as a downloaded song from an Internet site, and has selected this subset of the data set for presentation to a rendering device. The rendering device includes a security system that is configured to prevent the rendering of the select material if it can be shown that the user does not possess an entirety, or a substantial majority, of the data set.

The rendering system communicates a request for a particular segment of the data set, which is received by the substitution system of this invention, at 210. As noted above, the security system of the rendering system is designed to verify the presence of the entirety of a data set, and does so by requesting select segments of the data set, including segments beyond those of the material that is selected for rendering. If the requested segment is not part of the selected material, that is, not part of the material that was 'ripped' from the data set and downloaded to the user system, the substitution system accesses a dictionary that identifies the watermark that is associated with the requested segment, at 220. The substitution system then determines whether an authentic watermarked segment having this particular watermark is present in a collection of watermarked segments, at 230. If, at 235, a watermark segment having the appropriate watermark value is available in the collection, it is sent to the rendering system as the requested segment, at 240.

As is common in the art, a watermark verification system is configured to read a watermark from a segment of content material, and to then verify that the watermark has not been damaged, or modified, and to then verify that the information value of the watermark corresponds to a particular value. In the sample substitution system of this invention, the segments in the collection are segments that have authentic watermarks that have not been modified, and therefore the security system is overcome merely by providing segments that have the proper watermark value. Because the requested segment is not part of the material that has been selected for rendering, providing a bogus segment that merely has the appropriate watermark value has no effect on the rendering of the requested material.

If, at 215, the requested segment is part of the material that is selected for rendering, the requested segment is sent to the rendering system. Because the segment that is sent to the rendering system does correspond to the requested material, the rendering of the requested segment by the rendering system will provide the intended result. That is, if the select material is a song from a CD, providing the segments of the song from the select material that was ripped from the CD will result in the select song being rendered.

To increase the likelihood of a requested watermark being available in the user's collection of watermarks, the substitution system is configured to add the segments from the select material to the collection, if the watermark of this segment is not already contained in the

collection, at 260. Alternatively, all segments of the latest ripped material may be stored in the collection, replacing or augmenting prior segments that have the same watermark, so as to vary the response of the substitution system to subsequent requests for the same watermark.

If, at 235, the requested segment is not part of the material that is selected for rendering, and the appropriate watermarked segment is not available from the collection, the substitution system either ignores the request, as illustrated in FIG. 2, or may provide a segment with an erroneous watermark. If the security system is configured to allow for some degree of error in the watermarking process, returning a segment with an erroneous watermark may increase the likelihood of the substitution system of this invention overcoming the security system of the rendering system.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within its spirit and scope. For example, although the invention has been presented as a system that includes a predefined dictionary 120, the dictionary 120 for each particular data set may be downloaded at the same time that the ripped segments of the data set are downloaded. That is, the download of a selected song may include the watermarks of the segments before and after the selected song on the original CD. This set of watermarks, and the watermarks of the selected song, form the dictionary 120 for this CD. These and other system optimization and configuration options will be evident to one of ordinary skill in the art in view of this disclosure, and thus are within the spirit and scope of the following claims